Bob, it is Bob!

A short polemic addressed to IT experts: These may know something about privacy but nothing about dataprotection![1]

Martin Rost

For the past twentyfive years, IT experts have been taking a self-assured and enlightened stance to demand that non-technicians show more interest in the notorious insecurity of IT and the inadequacy of data protection. However, many articles do not justify this self-confident gesture because the authors often lack analytically significant knowledge on data protection - in contrast, for example, to topics of IT security. In many cases you understand data protection to mean only the protection of personal data. And then the question arises as to what personal data actually is. But what exactly does "data protection" mean?

The often observed incompetence of IT specialists with regard to data protection is a serious problem, especially when we say that avant-garde IT specialists see themselves also as political avant-garde, when they comment, for example, on logical contradictions, lack of expertise, short-sighted decisions. Violations of fundamental rights are often listed and highlighted on blogs, on Twitter, in traditional print media, but scandalization alone is no substitute for serious theoretical discussion of the subject of "data protection". But a serious examination of "data protection" is also not limited to a detailed orientation in the complicated data protection law. It has long been my suspicion that outrage activism, which however pervades the entire data protection scene, conceals the lack of serious analytical or theoretical discussions on data protection.

I would also like to simulate this self-assured, enlightened gesture, turn the tables and demand more serious interest in data protection from seriously politically interested IT professionals.

I would ask you to answer two questions yourself before reading on:

1) Which central conflict should be regulated by "data protection law"?

2) What is the difference between data protection measures and IT security measures?

Please make a note of your answers, perhaps with just a few rough keywords. Then you can see for yourself how conclusive your knowledge of data protection is.

[1] https://www.maroki.de/pub/privacy/2019-1124_itis_bob_polemic_Rost-v1.pdf
This article is based on a text first published in: "Bob, es ist Bob! in: FiFF-Kommunikation, 34. Jahrgang, Nr. 4: 63-66." http://www.maroki.de/pub/privacy/2017-12_fiff.html
This article was translated with the fabulous translation tool deepl (www.deepl.com) and then revised twice from myself. That won't be enough to minimize the German sound of the text. I would be very very grateful if a native speaker would revise this text, please ask for a copy. The deal could be that I rework a text translated into German. (2019/1124)

Thesis 1: Data protection does not take the protection of privacy as the starting point of the provision, neither does the protection of freedom, autonomy and self-determination of a person. Nor does the protection of the rights of those affected and, even less so, any notion of privacy, which can sometimes be so or so and sometimes also completely different or not at all, form the origin of data protection. And even the difference "public/private" does not create the essential data protection conflict.

Rather, data protection takes as its starting point the power asymmetry between organizations and individuals that creates risks. The data protection law and the technical and organizational data protection activities are already forms of the setting of conditions (conditioning) of this structural power conflict in modern societies. In the following I would like to explain the role of law and technology for this conditioning of power asymmetry, which is necessary in the rule of law.

On the one hand, there are the powerful organizations as risk givers - here, paradigmatically, one first thinks of the state, of course, but not only. On the other hand, there are those who are dependent on organisations and who are burdened by the organisations with the role of risk takers. Risk means here: Organizations generate disadvantages through the personal procedures they operate, which would not exist without these procedures for the persons. This conflict between organizations and individuals is the origin of the regulatory idea of data protection law.

In the early days of the 1970s, data protectors were primarily concerned with the state; today, it is primarily global companies that are not slowed down by any Leviathan. There is still no talk of technology at all. Was this crystal-clear idea of conditioning power asymmetry between organisations and individuals as an object of data protection law an answer that crossed your mind or did you perhaps even write it down? No? You see! Yes? Then I welcome you to Level 2, which follows immediately.

What does "conditioning of power asymmetry" mean?

The Rule of Law Promise, which is expressed and operationlized in data protection law, is that the relationship between any organisation and its associated persons is or may be subject to conditions. This relationship between organisations and individuals should not be "natural", but should be accessible in a legally and operationally reasonable way. For a reasonable form of relationship between organisations and individuals, organisations must, of course, know the generalisable criteria on the basis of which they must develop their procedures. These criteria contain the laws and then find their ultimate hold in fundamental rights. If people are at the mercy of the organizations that collect and process their data, such as Facebook, Google, Apple, Microsoft, Cisco, IBM, Akamai, Telekom, Vodafon ... for example, and citizens at the mercy of the public administration and the security authorities, or patients at the mercy of the hospital, then this is a special social, historical construction. Which could always turn out differently, both legally and procedurally or technically. Data protection checks such constructions of the organizations against persons on the basis of the requirements of the constitution, not on the basis of "informed consent". In this respect, data protection refers to all those precautions that organizations must take to shape the asymmetry of power between organizations and individuals in such a way that individuals are protected or can protect themselves from the arbitrariness of the organizations.

The idea that individuals can control their data and identities themselves without anchors in organizational processes is not, for example, an idea covered by data protection law. It is also factually nonsensical. Ideas on "self-data protection" have been discussed in the professional data protection scene in the context of "privacy enhancing technologies" since the end of the 1990s. Self-data protection in relation to IT is a pure fiction, because a user is always dependent on the use of already functioning technologies, which are ultimately produced or provided by organisations. It is impossible for private self-protection from violent organizations to be effective across all IT system layers. In this respect, a security anchor can only lie in the social structures, not in the people, not in the technology itself. Data protection must therefore, equipped with a social structural perspective, primarily work towards protective precautions for persons on the part of the organisations. And that is against the interests of the organisations. Data protectors who do not create conflicts are therefore not data protectors.

In the shadow of a strong state that grants basic and civil rights, in principle eye level can be established between all addressable units of a state. A strong state is both the only guarantor of the effective enforcement of fundamental rights and the strongest attacker of the very fundamental rights it grants. Are you familiar with this dialectic of such a simultaneity of the role of guarantor and attacker of the state? To take another example of this dialectic... think of the doctor-patient relationship: no one can kill you as legally as doctors if, for example, you are seriously injured or if you are to have surgery, but they are the only ones who will let you survive.

Privacy and informational self-determination, which of course play an essential conceptual role in data protection, are characteristics of social relationships, but they can only develop if organisations have not previously acted in a way that encroaches on individuals. If few organizations "shape" people's lives directly - organizations are not drawn into a check & balances - then this is sociologically the central indicator for a pre-modern society. The organizations of a society with their specific constraints are always there, no matter what need for autonomy, privacy and rebellion people feel inwardly. In this respect, privacy for everyone and the demand for self-determination are characteristics of social structures that can only emerge historically under preconditioned circumstances. They characterize the very latest modernity, which is concretely characterized by "functional differentiation" (Niklas Luhmann). This functional differentiation of social systems, in which there is no logical order of things from one point out, forces people to act in the mode of self-determination with the "compulsion to individualization" (Norbert Meuter) - a mode that nobody in modern societies can freely choose to adopt. What is meant by "coercion to individualization"? There is no dress code today, except in emphatically authoritarian organizations. As a citizen one chooses political programmes or persons and marries according to one's own convictions and feelings, one chooses a suitable one in Abu Dhabi from among 3,000 different courses of study; one can try to be simple and sensual or to emphasise one's body or to invest in the training of one's wit, intellect, spirituality or taste. How people shape themselves is therefore openly contingent. But the fact that in these and a large number of other parameters one has to arrive at solutions to the shaping of one's life, which then inevitably lead to a unique constellation for each person, is not optional in modernity. There is an obligation to select. How can organizations then still presume to intervene in the shaping of life? But that is exactly what organisazions are doing, again more than ever. Claiming individuality is thus as little a private matter as data protection is not.

I'd like to ask you a question: What exactly is meant by the aforementioned "fundamental rights"? Yes, exactly, fundamental rights, in contrast to human rights and civil rights? This is the type of rights that is typically dealt with in the first semester of a law degree course, i.e. the type that forms the yardstick for the analysis and assessment of data protection requirements, e.g. the Data Protection Basic Regulation

(DSGVO). Make a note of your answer to this question! What are fundamental rights and how do they differ from other rights? I will not give you the answer here.

But there is another intermediate question: What is without any doubt the CENTRAL REGULATION in continental European data protection law? You do not understand what the question is about? Are you surprised that there is such a thing as THE ONE central rule in this juggernaut of the 99 articles of the DSGVO? If the answer comes to your mind, which I very much hope it will, then perhaps you will also be able to name the article from the basic data protection regulation? This central rule is undoubtedly as clear and without alternative as the Deny All rule of a firewall administration. I will not mention this article of the DSGVO to you either.

But there is another question: Do you know the wording of the first article of the EU Charter of Fundamental Rights? My experience from a large number of data protection training courses in recent years shows that many experts on questions of IT security and data protection are unable to answer these three simple questions on data protection and data protection law. It is true, of course, that citizens must be required to have more knowledge of IT security, but politically committed IT specialists and computer scientists must also be required to have concrete knowledge of fundamental rights and their effective implementation through data protection law. The practice does not only consist of technology, business administration and a few political views.

You can now again see from your activities how serious you really are about data protection when you start researching (or not researching) the missing answers to the above questions. If you get caught up in the EU Charter of Fundamental Rights on this occasion, take another look at Article 7 and especially Article 8.

So now back to the question announced at the beginning about the difference between operational data protection and IT security. How about a few rough notes in which you note the difference between operational data protection and IT security? I won't owe you an answer here.

Thesis 2: The starting point for operational data protection is not the notorious and obvious insecurity of IT, which may be used in the processing of personal data. Instead, the starting point for operational data protection measures is the intensity of intervention in an organisation's personal data processing. Questions of IT security or the systematic exploitation of technical weaknesses by organisations only arise in the second place. First and foremost, any processing of personal data by an organisation constitutes an encroachment on a person's fundamental rights.

It is easy to read over the previous sentence, for example in "yes yes is clear" mode. However, you should not do this; please read it again. This sentence contains the paradigm of operational data protection.

To put it another way: The mere fact that personal data are processed creates a risky asymmetry of power to the detriment of the person concerned. This is the conflict to which serious data protection must respond. Operational data protection therefore focuses on those protective measures that are intended to reduce the intensity of intervention - or the degree of impairment, as stated in the basic data protection regulation that will apply from May 2018 - in data processing. These include, for example, techniques with the help of which data processing can be (re-)checked, particularly with regard to the effectiveness of protective measures. How is verifiability - i.e. an accounting of target specifications, which can be found in the law, and actual findings, which result from the observation of process characteristics - established in data protection? A procedure, and the data processing used for this purpose, must be specified with regard to the establishment of testability (directed towards the future of the procedure), must be documented with all data, IT components and processes (identification of the method for determining the actual states of the procedure with reference to the target values) and the procedure must be recorded (directed towards the past). In addition, this includes techniques which, above all, functionally limit the purpose of data processing by drawing in boundaries, e.g. by distinguishing between individual procedures and their respective databases, IT systems or processes, and which are only used in a manner closely oriented to the purpose.

The transparency or verifiability of a procedure is not an end in itself, because transparency alone does not have a protective effect on data subjects. Verifiability creates transparency in order to be able to assess whether the measures to reduce the intensity of intervention are adequately effective. An example of such a measure to reduce an intervention intensity is the setting of limits for a procedure or its data processing. What does "delimit" or "separate" mean? And how permeable does a "limit" for a procedure have to be anyway?

Let's assume that you have the three powers - the three powers you have on you, I have no doubt about that now - calculated in the same computer centre of a country. The fact that the various powers rely on a common IT infrastructure is now common practice, although a data center - you can also think of clouds as an alternative - forms an operational short circuit between the powers. For example, the Enterprise Service Bus (ESB) from Microsoft can be used in a clearing house or another architecturally central location for the central switching of data packages. From a data protection perspective, the question that arises in view of such a switching architecture, which is used in a procedure, is: Can the specification, documentation and logging of the ESB be used to check how the separation of powers is ensured? Or to put it more generally: Which system boundaries are effective on which layer of a procedure? At a national data center, such aspects can at least still be checked, but with typical cloud solutions, nothing more can be checked in this respect. Once again, it becomes clear that the starting point for data protection is the conditioning of power asymmetry, which must not be undermined at the operational level and which does not affect any typical IT security problems.

So, and what about IT security? In the meantime, colleagues from IT security management are taking care of potentially attacking hackers. IT security management rose to become a powerful department within many organizations a good ten years ago. Few organization managers still have to be told that their organizations have crown jewels that they should protect. And they now also know how insecure the operation of IT is. The security measures then focus on the security of business processes, not on the security of those affected by the activities of the organization itself. Outside the critical infrastructures (for Germany the keyword is "KRITIS"), organizations are not legally obliged to operate a secure IT system, apart from for reasons of data protection! If an organization's management then blocks itself and does not want to provide funds, the IT security officer sometimes has to refer to data protection laws. With the consequence that then security measures, which do not serve the protection of the concerning, are operated. Within IT security, the protection of those affected is at best listed as a compliance risk. This means that organizations are only interested in data protection to the extent that they calculate the costs associated with data protection violations (and how great the risk is that these violations will be detected, for example, by a data protection supervisory authority). Therefore, as a data protector, you have to repeatedly explain to the IT security officer in particular that protection must apply first and foremost to those affected and that IT security measures must therefore also satisfy the fundamental requirements for reducing the intensity of intervention. In this respect, it is undoubtedly true:

Basic legal data protection measures must dominate IT security measures! But have you ever tried as a data protector to talk about this conflict with the organisation management or an IT security officer?

One thing is clear: a data protector who has no conflicts is not doing his job. No matter whether in the company or as a public data protector. Because the organization you work for as a data protector or deal with is ... the main attacker. Of course, this remains an organization even in a legally compliant company, where, exceptionally, the consent of those affected is not a farce and where IT operations may also have good information security. However, many operational data protection officers, simply because their tasks are not clearly in front of their eyes, offer themselves to their organizations as sidekicks of the security officers.

What follows from all this theoretically and politically? In the following I will address three typical theses, which I will comment on in the light of the above.

For example, it follows from the recognition of the power asymmetries generated by organizations that algorithms themselves cannot be to blame for anything if something goes wrong or goes wrong. It is always the organizations (not even the individual employees) who create the algorithms, from simple artefacts to networked-complex artificial intelligence (AI), and who thus charge their personal inventory with motifs and thus create any "relationship of obligation" at all. Technology helps organizations to reproduce, consolidate and expand power asymmetry.

The talk of algorithm ethics or data protection ethics throws very nasty wafts of fog. The assumption that one simply cannot know how to contain new technologies due to a strong technical change, and the resulting recommendation that one therefore prefers to try cloudy ethical discourses - instead of implementing valid law in the best possible way - serves solely and exclusively the interests of the strong organisations, which are hindered by fundamental rights and data protection. Permanent monitoring of people by mobile phones or listening assistance systems in their homes is not compatible with the EU Charter of Fundamental Rights, and effective supervision of data protection would also detect this. If the interference with fundamental rights by a procedure cannot be minimised to a level acceptable under fundamental rights by protective measures, the procedure must not be used by the organisation. Those who recommend ethics for the normative regulation of such data protection conflicts undermine the existing data protection law and this benefits the organisations. The motives of the organisations that develop and use such invasive techniques do not change at all, but on the contrary are cemented better than ever by the use of new techniques. And these are the activities on which data protection law is based: organisations are still and will continue to be concerned with stabilising an optimum return on capital, including through the power of disposal over individuals. It is still a question of maintaining and increasing power with regard to the establishment of public order or of truth constructions that nobody should be able to ignore. Data protection law aims to ensure that no natural forms of rule are enforced en passant with the help of technology that undermines democracy, the rule of law, the market and free discourse.

And even the demand for data sovereignty, which somehow seems correct, with the idea that "my data belong to me" only shows that not fundamental rights but property and market mechanisms provide the frame of reference, as if citizens were only customers who must have one thing above all else: The choice. But it is not about election, but about the pacification of notoriously violent organisations. And the state is the regulatory body for this. This change in the prioritization of goods over standards also plays into the hands of the dominant organizations, again at the expense of those affected.

What needs to be done? Since 2012, around a dozen colleagues from the Technology Working Group of the Conference of Data Protection Officers of the Federal Government and the Countries (Germany) have been developing the Standard Data Protection Model (SDM). The 68-page handbook on the model has been available on the websites of almost all data protection supervisory authorities in Germany since November 2019. On the one hand, the SDM offers a methodology for communicating legal norms and technical functions and, on the other hand, offers the prospect of a catalogue with specific standard data protection reference measures.

For anyone who is seriously interested in data protection, it can therefore be clear for what reasons which measures for the enforcement of data protection are to be taken. And again, you can see the seriousness of your interest in effective data protection by whether you are researching SDM (or not).

In the end, it turns out that not only Alice and Bob have to protect themselves from Carol when it comes to data protection, but Alice also has to be protected from Bob if she cannot effectively protect herself from Bob alone, because Bob is structurally incomparably stronger from the outset.